ATTORNEY DOCKET NO. BIODONGLE/SCH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Scott C. Harris Art Unit: 2131
Serial No.: 09/712,398 Examiner: H. Mahmoudi
Filed : November 14, 2000
Title : SOFTWARE SYSTEM WITH A BIOMETRIC DONGLE FUNCTION

Mail Stop AF
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPLICANTS BRIEF ON APPEAL

Sir:

Applicant herewith files this Appeal Brief under 37 C.F.R. 41.37, thereby perfecting the Notice of Appeal that was originally filed on January 17, 2004. The sections required by the rules follow.

The present application qualifies for small entity status under 37 C.F.R. § 1.27. Please charge the $170 fee for the Appeal Brief and a $60 one month extension fee to deposit account 50-1387.

Real party in Interest

The inventor, Scott C. Harris, remains the real party in interest.

CERTIFICATE OF FAX TRANSMISSION

I hereby certify that this correspondence and all marked attachments are being facsimile transmitted to the Patent and Trademark Office on the date shown below:

4/19/05
Date of Facsimile

Scott Harris
Signature

Scott Harris
Typed or Printed Name of Person

Related Appeals and Interferences

There are no known related appeals and/or interferences.

Status of Claims

Claims 3-14 remain pending. All of the pending claims are appealed.

Status of Amendments

An amendment after final was filed on November 15, 2004. An advisory action indicated that this amendment would be entered.

Summary of Claimed Subject Matter

Claim 3 requires a special kind of computer program that stores encrypted information. An encrypted sequence is stored during installation. See generally page 8. Personal information is obtained as part of the startup sequence for a computer program. This may be biometric information, see generally the bottom of page 12. The obtained biometric information is compared against the previously stored information, see page 13 lines 9-11. The computer is allowed to run at 430 if there is a match, see page 13 lines 14-15. Claim 3 further requires that the installation of the computer program includes entering the biometric code, sending that code to a server, and returning an encrypted sequence as encrypted information. This is part of the installation described above, see generally page 8.

Claim 7 similarly requires storing the encrypted information (see generally page 8), obtaining personal information as part of the startup sequence (see the bottom of

page 12), comparing the personal information (page 13), allowing the computer to run normally if the information agrees (page 13), but allowing a limited exception mode without establishing that the personal information agrees with the decrypted information. This is described on page 11 line 19 through page 12 line 4, where the limited run or "exception" mode is allowed.

Claim 8 requires installing a computer program, requesting the system to install, see page 5 beginning line 6, verifying whether the computer program is verified for installation, see generally first paragraph on page 7, obtaining a reference biometric from the user see page 8 lines 9-16, and thereafter allowing execution of the program only if the entered information matches the reference biometric see generally page 8 lines 17-19 and other locations within the specification.

Grounds of the Rejection to be Reviewed on Appeal

Claim 7 is rejected under 35 U.S.C. 102b as allegedly being anticipated by Applebaum. Claims 8-14 are rejected as being anticipated by Brody.

Both of these rejections are appealed herein. All of these rejections are respectfully traversed.

Argument

The rejections under 35 U.S.C. 102

Claim 7 rejected under 35 U.S.C. 102 as allegedly being unpatentable over Applebaum. With all due respect, it is suggested that this rejection is in error.

First, and prior to discussing the rejection, consider what is claimed by claim 7. Claim 7 defines storing encrypted information associated with a computer program, obtaining personal information as part of the start up sequence, reading the encrypted information and decrypting it to obtain decrypted information and comparing that personal information with the decrypted information, allowing the computer program to run normally only if the personal information agrees with the decrypted information in a specified way, and finally allowing the software to run in a limited exception mode without establishing that the personal information agrees.

Applebaum discloses an Internet appliance. The user is required to give biometric information see generally paragraph 52, to log on to that internet appliance. Alternatively, the user can identify themselves some other way. Encryption may be used to make the security more complete.

However, Applebaum describes the information appliance verifying the identity of the user, and after identifying that identity, the information appliance "can communicate with the computer 306 and the server 310". See column 52. Applebaum therefore simply describes using biometrics prior to communication – effectively as a security protocol for the communication. Nowhere is there any disclosure that the biometric identification is done as part of a startup sequence for a computer program as claimed. Moreover, nowhere is there any disclosure that the program only runs normally only if the personal identification agrees. Applebaum allows communication, not running a computer program as claimed, once the user identifies themselves. As explained in paragraph 56, an information appliance can be secured in this way.

This discloses nothing about the claimed startup of a computer program, and allowing the computer program to run normally only if the personal information agrees. Moreover, claim 7 requires a limited exception mode and further allows "the software to run in a limited exception mode without establishing that the personal information agrees" (emphasis added). The rejection refers to claim 36 of Applebaum as supporting this. Claim 36, however, simply states that the identification is compared and that access is allowed if it matches, and that access is 'restricted' if the personal information does not match. There is no disclosure of any limited exception mode in Applebaum. Claim 36 of Applebaum simply states restricting access. Restricting access is well understood: the user can not obtain access. Moreover, note that Applebaum discloses communication being allowed if the security matches; there is no disclosure of any limited communication mode in Applebaum. The patent office's rejection on this basis is pure conjecture, not supported by Applebaum. There is no disclosure that the software is allowed to run in a limited exception mode without establishing that the information agrees. There is only the disclosure of "restricting the access". With all due respect, it is respectfully suggested that this rejection is based on hindsight, and not on the disclosure of Applebaum. Quite simply, Applebaum discloses nothing about any limited exception mode being entered at all. All it discloses is that the access is restricted.

Claims 8-14 stand rejected under 35 U.S.C. 102b as allegedly being anticipated by Brody. This contention is respectfully traversed. Claim 8 recites requesting a computer system to install a program and determining whether the program is verified for installation. Claim 8 recites obtaining "a reference biometric at the time of installing the software responsive to said determining...".

Therefore, this claim requires : a) determining whether the program is verified, and responsive to that determining, b) obtaining a reference biometric. Therefore, any user can install the software, but, whoever that user is, they must provide the program with a reference biometric at the time of installation. After installing, claim 8 recites that the program is allowed "to run normally only when biometric information is obtained which matches said reference biometric".

This is a very different system than that disclosed by Brody. Brody requires that each piece of software is "individually personalized for each customer separately to include personal information of the customer..." see for example paragraph 147 of Brody. Nowhere is there any disclosure of obtaining this information as part of the installation routine. Rather, Brody requires that each copy of the software is individually personalized when made. In contrast, the present system is individualized only when installed. That is, the software, when made, can be used by any person.

Brody admittedly discloses encryption and decryption in paragraph 152. However, note that the information is authenticated "prior to or during the software build". The verification of the personalization is at run time, but the individualization is carried out during the software build, see generally the beginning of paragraph 152.

Therefore, Brody only allows installation of the software by the person for whom the software was personalized. In contrast, claim 8 allows anyone to install the software. However, once installed, the software is matched with a reference biometric, and cannot later be used by anyone who does not match the reference biometric. This is different than Brody, and is nowhere disclosed by Brody.

Claim 9 is even further allowable, as it requires determining if the specified license has already been used. This would appear to be unnecessary in Brody who personalizes each copy of the program. Similar arguments apply for claim 10.

In rejecting claim 10, the rejection points attention to paragraphs like paragraphs 10 and 15 which describe how the prior art has recorded a unique serial number. However, Brody discloses personalizing each copy of the software, and therefore effectively discloses away from using such a unique serial number. Admittedly, Brody discloses finding and generating a unique identifier, but discloses nothing about using this to install the software so that the user's biometric information can be obtained at the time that the software is installed, as claimed.

Rejections Under Section 103

Claims 3-6 stand rejected over Applebaum in view of Brody. This contention is respectfully traversed.

First of all, a person having ordinary skill in the art would not be motivated to make an operative combination of Applebaum in view of Brody. Applebaum teaches a very different system than Brody. Applebaum's system relates to an Internet appliance. Brody's system relates to individualization of software copies to specific individuals. Applebaum allows access to an appliance, not to a computer program. Applebaum teaches that biometric information can be obtained from the user and compared with biometric data that is stored, to verify an identity. Paragraph 56 describes that encryption can be used. The encryption can avoid broadcasting the identity of the user throughout the network. Other encryption is described in paragraphs 54 and 55.

Paragraph 54 describes that the encryption is carried out using the private key held by the server and that a public-key is provided to each user. However, nowhere does Applebaum have any teaching or suggestion of using his encryption scheme for use in determining whether a computer program can be executed. This has simply never been suggested by the prior art.

A person having ordinary skill in the art would not be motivated to combine these two references. There is quite simply no connection between the two. An Internet appliance would not be considered to provide any guidance to a person having ordinary skill in the art about what to do during software installation, and vice versa. Therefore, the hypothetical combination of these references is based on hindsight and the teaching of the present specification, and not on the teaching of the references themselves.

Moreover, even if the references were combined, the hypothetical combinations still would not teach or render obvious claims 3-6. Neither reference teaches or suggests the use of personal information "as part of the startup sequence for said computer program ". As noted above, Brody teaches individualizing the software, not the use of personal information to decide if the software can run. Neither reference teaches allowing said computer program to run normally only if said personal information agrees with said decrypted information in a specified way ", where the personal information is biometric information, and the computer program is installed by entering a biometric code, sending that code to a server, encrypting the code at the server and returning it. Quite simply, this combination of subject matter is not taught or suggested by the cited prior art, even if combined.

Moreover, it is respectfully suggested that the only thing suggesting making this hypothetical combination in the first place is the teaching of the present specification. As extensively discussed above, both Applebaum and Brody teach very different subject matter, and the hypothetical combination is made only based on the present specification's teaching.

Therefore, and with all due respect, the Examiner's decision of unpatentability should be reversed.

Please apply any charges not covered, or any credits, to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 4/19/05

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082

Appendix – All Claims on Appeal

3. A method, comprising:

storing encrypted information associated with a computer program;

obtaining personal information as part of a startup sequence for said computer program; and

reading said encrypted information, decrypting information contained therein to obtain decrypted information, and comparing said personal information with said decrypted information;

allowing said computer program to run normally only if said personal information agrees with said decrypted information in a specified way;

wherein said personal information is biometric information, and said comparing comprises comparing said biometric information with other biometric information in said encrypted information, and

further comprising installing said computer program by entering a biometric code, sending said biometric code to a server, encrypting said biometric code at said server and returning an encrypted sequence to said computer program as said encrypted information.

4. A method as in claim 3, wherein said encrypting uses a private key at said server, and said decrypting verifies a signature of said private key.

5. A method as in claim 3, wherein said encrypting uses a private key at said server, and said decrypting uses a public key included as a part of said computer program.

6. A method as in claim 3, further comprising determining if a biometric reader is attached to a port, and wherein said program is only allowed to run if said biometric reader is attached to said port.

7. A method, comprising:

storing encrypted information associated with a computer program;

obtaining personal information as part of a startup sequence for said computer program; and

reading said encrypted information, decrypting information contained therein to obtain decrypted information, and comparing said personal information with said decrypted information;

allowing said computer program to run normally only if said personal information agrees with said decrypted information in a specified way; and

further comprising allowing the software to run in a limited exception mode without establishing that said personal information agrees with said decrypted information.

8. A method, comprising:

requesting a computer system to install a specified computer program;

determining whether said computer program is verified for installation;

obtaining a reference biometric information from an authorized user at the time of installing the software, responsive to said determining that said computer program is verified for installation; and

thereafter allowing said program to run normally only when biometric information is obtained which matches said reference biometric information.

9. A method as in claim 8 wherein said determining comprises determining if a specified license used for said installation has already been used for another installation.

10. A method as in claim 8 wherein said determining uses a specified unique code that was distributed with the program, and determines from a server whether said unique code has already been used for an installation.

11. A method as in claim 8, further comprising, after determining that said installation is authorized, sending said reference biometric information to a server.

12. A method as in claim 11, further comprising, at the server, encrypting said reference biometric information, and returning encrypted biometric reference information which is stored with said program, and which is used by said allowing.

13. A method as in claim 8, wherein said allowing retrieves encrypted biometric information, decrypts said biometric information, and allows said program to run normally only if said decrypted biometric information matches a currently entered biometric information.

14. A method as in claim 12, wherein said reference biometric information is encrypted at said server using a private key of a public key-private key pair, and said reference biometric information is decrypted when software is to be run, using said public key corresponding to said private key.

ATTORNEY DOCKET NO. Biodongle/SCH
Serial No.09/712,398